Vermont Department of Health

Vermont WIC MIS/EBT Planning

Security Plan

Version 1.1

Revision History

Date	Version	Description	Author
11/4/11	1.0	Draft Created	Nancy Rowell
12/15/11	1.1	Updates after K. Rowley State Security Review	Nancy Rowell

Table of Contents

.

Security Plan

1 Vermont WIC MIS including EBT Delivery System

Vermont WIC Management Information system including Electronic Benefit Transfer Delivery System is comprised of:

- MIS System
- MIS-EBT Interface
- External EBT System/Host
- System Messaging

2 Information System Categorization

The FIPS 199 categorization ID for the MIS, i.e., catastrophic loss

- For the MIS and EBT is high if a Secretary of State "Safe at home" participant's demographic data is compromised
- For the MIS and EBT is low for specific prescription data
- For the MIS is high for a participant's personal health data.

3 Information System Owner

Vermont WIC Program, Maternal Child Health Unit, Vermont Department of Health, Agency of Human Services, 108 Cherry Street, Burlington, VT 05401, wicvt@state.vt.us, (802) 863-7508

4 Authorizing Official

Donna Bister, Donna Bister, Child Public Health Administrator, Vermont Department of Health, Agency of Human Services, 108 Cherry Street, Burlington, VT 05401, donna.bister@.state.vt.us, 802-863-7508

5 Assignment of Security Responsibility

Kris Rowley, Chief Information Security Officer, Department of Information and Innovation, Office of Information Security,133 State Street, Montpelier, VT 05602, Phone: 802-828-0911, Fax: 802-828-1244, Email: kris.rowley@state.vt.us

6 Information System Operational Status

The operational status of the system is currently in Planning with Development/Installation to occur as soon as possible.

7 System Type

- The WIC MIS system is a Management Information System application
- The WIC EBT system is a benefit delivery and management system

8 General System Description/Purpose

Information Systems (IS) in the Special Supplemental Nutrition Program for Women, Infants and Children (WIC Program) support a number of program operations and management functions. The MIS/EBT system contains all business process, which certifies Vermont WIC participants, assigns benefits; transfers benefits and supports benefit redemption including the following:

- Appointment Management
- Caseload Management
- Certification
- Financial Management
- Food Benefit Issuance
- Food Benefit Redemption, Settlement & Reconciliation

- Nutrition Education, Health Surveillance & Referrals
- Operations Management
- Scheduling
- System Administration
- Vendor Management

The Functional Requirements Document for a Model WIC System (FRED) provides a comprehensive description of functions that are included in the WIC MIS. http://www.fns.usda.gov/apd/WIC_FRED.htm

The approximately 160 Vermont state users and their user environments are varied. The user community ranges from Public Health Nurses at remote Clinic locations to the super users within VDH who must report to a federal level.

9 System Environment

The hardware system environment includes multiple locations for the WIC MIS and EBT. The central MIS hosting location at DII, the WIC Administrative site at the Vermont Department of Health and Clinic locations within State District Offices are all within state network control. Remote clinics in public facilities, the externally hosted EBT system and retail grocer locations throughout Vermont and including retail border grocer locations in New York, Massachusetts and New Hampshire function external to the state network.

The software includes development, test, and production environments.

10 System Interconnections/Information Sharing

The systems below represent systems, which either require information from or send information to the WIC MIS system. None except the EBT systems are truly integrated and the data exchanges could be more accurately classified as data import/exports.

System Name	Organization	Type	Agreement (ISA/MOU/MOA)	Date	FIPS 199 Category	C&A	Status	Auth.	Official
Medicaid	AHS				High		Planning		
CIS	AHS/DCF	Export			High		Planning		
IMR	AHS/VDH IMR	Import			High		Planning		
HHLPSS	AHS/VDH Lead	Import			High		Planning		
SNAP	AHS						Planning		
EBT Host	TBD	Messaging			High		Planning		
NUPC DB	USDA/FNS	Import			Low		Planning		
Medical Providers	VITAL				High		Planning		

11 Related Laws/Regulations/Policies

11.1 NIST

The system must comply with security controls for moderate impact information systems as put forth in NIST Special Publication 800-53, Revision 3, as updated May1, 2010

11.2 Safe At Home

The system must implement standards to protect and guard against the misuse of individually identifiable health information held or transmitted in any form or media, whether electronic or paper, at the record level.

11.3 HIPAA

Health Insurance Portability and Accounting Act of 1996

- Using Authentication controls (user ID and Password)
- Encrypting protected Health information (PHI) on the database and during transmission
- Having in place a comprehensive disaster plan
- Restrict access to PHI to staff who need it in order to perform job duties
- Intrusion detection capability
- Administrator defined timing out of workstations to prevent unauthorized viewing of PHI

11.4 Established Policies

All established policies, procedures, and guidelines, whether they have been invoked by the USDA FNS, VDH IT, VDH, AHS, DII or State of Vermont policy

12 Central Hosting Facility

12.1 SOV Security Policy & Procedures

12.1.1 Introduction

There are two types of security to consider. Access to the State of Vermont's information systems and computing resources will be based on each user's access privileges and a user will be authenticated through Active Directory. Access privileges will be granted on the basis of specific job needs (i.e. a "need to know" basis). Access controls must ensure that even legitimate users cannot access stored information unless they are authorized to do so. All applications will have access controls unless specifically designated as a public access resource.

State of Vermont IT employees are responsible for maintaining secure access to the State of Vermont information systems and computing resources. Access permission levels will be determined by individual departments/agencies as employee supervisors deem appropriate.

The second is application-only. Security includes a user ID and password controlled by the application and based upon role based security.

12.1.2 Requirements

To support the Information Vermont State Security Policy, the following requirements are defined:

- Terminated employee, contractor, and vendor user accounts to all applications, systems, resources and physical access will be revoked, disabled and terminated immediately following exit.
- State of Vermont information must be protected from unauthorized disclosure, modification, or destruction. Information about security standards and practices must be implemented to ensure that the integrity, confidentiality, and availability of information are not compromised.
- All hardware and software used by the State of Vermont will be documented and in compliance with all State applicable standards and policies.

- Documents that contain information that may be sensitive (i.e. SS#, HIPAA information, etc.) must be assigned a classification (confidential, private, public) in order to determine the level of sensitivity in which they must be handled.
- Personnel who have access to sensitive information may require background checks or screenings. Screenings and background checks will be conducted per department/agency and DHR policy.
- Restricted areas within agencies/departments that house sensitive or critical information systems will at a minimum, utilize physical access controls designed to permit access by authorized users only.
- To maintain the availability, integrity and confidentiality of information, computer and communications equipment will be secured from physical and environmental threats.
- System capacity requirements will be monitored and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.
- Agencies will establish internal procedures for the secure handling and storage of all electronically stored information that is owned or controlled by such agency.
- Users with access to State of Vermont customer sensitive information are strictly prohibited from downloading any customer information onto laptops, disk, flash drives, etc. unless the portable device is encrypted. Examples of sensitive information may be a combination of any of the following but not limited to this list:
    - Customer name
    - Mailing address
    - Email address
    - Phone number
    - Credit card information
    - Social Security Number
    - Health information
    - Banking Information

12.1.3 Data Centers

<u>DII Data Center Locations</u>

133 State Street, Montpelier
McFarland House, Barre
National Life, Montpelier
All locations are secure access facilities, not open to the general public.

The main data center at 133 State Street is provided with an uninterruptable power supply and back-up generator to ensure up- time in the event of a prolonged power outage. The data center at National Life is the newest center. It also provides an uninterruptable power supply and back-up generator. The data center at McFarland House in Barre provides limited space for disaster recovery of critical systems.

12.1.4 Physical Environment

<u>Power supply</u>

- Redundant UPS system
- Standby generator
- 24x7 power back up systems

<u>Environmental Control</u>

- Air-conditioned environment
- Temperature and humidity control and monitoring

Physical Security

- Electronic Key Access
- Multiple-zone access control
- Lockable cabinets and racks
- Unauthorized access alarm systems

Fire Suppression Systems

- Multiple zoned, pre-action dry pipe system

12.1.5 *Types of Services*

DII Technical Support Services offers a full range of information support through planning, evaluation, installation, tailoring, monitoring, diagnosis, maintenance, problem solving, training, security and administration of system control and third party programs. DII also provides database and data storage management services. The following services are relevant to the MIS/EBT system:

- Physical spaces for computers, servers, peripherals, networking, telecom and other equipment
- Server Hosting
- Backup and Recovery Solutions - Backups of servers and provide for safe storage and retrieval of all backup tapes and monitor for alarms. Backup and recovery services are provided by NetBackup, which can be managed by designated NetBackup System Administrators. The NetBackup application and database components are installed on separate Windows 2003 servers (Master & Multiple Media Servers), plus a HP MSL4048 2 Ultrium960 Tape Drive, in the SOV Enterprise NetBackup Environment, as part of an HP EVA 8000.SOV Enterprise Backup/Recovery Services provides a complete and flexible data protection solution for a variety of platforms, including Microsoft Windows, UNIX, Linux, and NetWare systems. Also included is the support for leading database engines like Microsoft SQL Server, Sybase and Oracle; providing near real time database protection. By carefully scheduling backups, administrators can achieve systematic and complete backups over a period of time, optimizing network traffic and application performance during off-peak hours. Benefits include: Lower client support costs by integrating and extending problem reporting and backup operations monitoring to client systems. Reliably and securely scales management responsibility across teams and infrastructure with role-based, more scalable architecture. Reduces IT management complexity by automating routine administration.
- Power and cooling for computers, servers, peripherals, networking, telecom and other equipment.
- Physical security for computers, servers, peripherals, networking, telecom and other equipment, as well as data storage devices such as disk and tape volumes
- Server Monitoring and Alerting - Monitoring and troubleshooting and customer support services, 6 AM-12AM, M-F. Monitoring and back up call support off hours. Monitor system consoles for performance, system errors and job failures. DII's server monitoring service utilizes Microsoft's System Center Operations Manager (SCOM) to watch primary domain servers. In addition to SCOM, DII also uses Solar Winds for system monitoring and threshold alerting for systems that are not within SCOM's domain boundary.
- Remote job operation services.
- Job scheduling, library, and quality assurance services.
- Server Antivirus and Multi-Tier Protection
- Server Maintenance, Patching and Updating
- Active Directory Services - Active Directory Services (ADS) is a manner to service all who login to a computer upon accessing the DII/SOV network. Authentication for the network is provided by AD. Also, AD lets the computer know whether the requestor has the access to

log on or not from any particular computer. ADS shares information to those who have the permissions to it. This includes printers throughout DII/SOV. After a successful authentication, ADS can shield sensitive data from unauthorized access.

- SQL Administration & Support
- Server Configuration Support (DNS, DHCP, WINS)
- Mobile Device Support

Software supported on DII enterprise servers:

- DFSMShsm (Hierarchical Storage Manager) is an optional feature providing backup, recovery, migration, and space management functions.
- RACF (Resource Access Control Facility) is IBM mainframe security software that verifies user ids and passwords and controls access to authorized files and resources.
- TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or extranet).
- Connet:Direct provides the capability for moving mission-critical data to and from a variety of platforms supporting multiple communication protocols.
- VTAM (Virtual Telecommunications Access Method) is an IBM application program interface (API) for communicating with telecommunication devices and their users.
- NETVIEW is IBM's network management system. A text message-based system that monitors, manages and controls SNA networks.
- TSO/ISPF is an IBM text editor and programming facility.
- QWS3270 is a standards compliant TN3270 emulator application.
- Zeke is an automated job scheduler and monitor.
- TMON offers detailed monitoring of operating system performance.
- CA TLMS Tape Management is an automated tape management system which controls and protects z/OS tape volumes and data sets.
- VM/ESA is an IBM operating system capable of running multiple systems, with each running its own programs.

12.1.6 Data Centers Access

The DII Data Centers provide a 24x7 high availability, redundant, and secure environment for all systems in compliance with HIPPA and other regulations as may exist.
The DII Data Centers are intended to enable systems administrators of the servers housed in a Data Center to be able to effectively manage their machines remotely and securely. All personnel must have proper authorization to obtain access to any of the DII Data Centers. Authorized individuals will have unassisted access to the DII National Life Data Center 24 hours a day. Every authorized individual will have National Life access cards assigned to them that will allow them entrance to the National Life facility when needed. The National Life access cards are issued by National Life, but preliminary authorization is granted by the DII Data Center management. The process to acquire authorization for each level is detailed below. All persons requesting access to the DII Data Center must have proper authorization. A Data Center authorization form must be on file for each person who is requesting authorization to enter. This file will be maintained by DII staff. DII will notify BGS Security to remove authorization of employee access if there is a job change or termination of employment or if there is found to be a violation of any DII Data Center rule.

<u>Visitor Guidelines</u>
Anyone who does not have an authorization card is considered a visitor. This includes state personnel without an approved authorization and all vendor staff. Visitors must be accompanied at all times by an authorized employee while in any DII Data Center. Visitors

must log in and out when entering and exiting the DII Data Center. The purpose of the visit must be documented as part of the log in process. All visits to the DII Data Center are scheduled through the DII Data Center Management at least 24 hours in advance. Please contact DII-DataCenterManager@State.vt.us to arrange for a visit.

Authorization Process

An employee requiring access to any DII Data Center must receive authorization by Data Center management. Please contact DII-DataCenterManager@State.vt.us to request authorization. Once approved, the employee's name will then be added to the authorization list and the employee will be given an access card.

Audit Procedures

- The Data Center Manager will send a list of authorized employees to each manager on a regular basis for review and verification.
- The manager will review and update the list of authorized employees and return it to the DIIDC Manager within two weeks.

12.1.7 Data Center Rules

- No food or drink is allowed within the DIIDC.
- No hazardous materials are allowed within the DIIDC.
- All packing material must be removed from computer equipment and/or components in the specified staging areas before being moved into the DIIDC. This includes cardboard, paper wrap, peanuts, plastic, wood and other such material.
- No cleaning supply is allowed within the DIIDC without prior approval. This includes water.
- Only HEPA filter vacuums may be used inside the DIIDC.
- No cutting of any material (pipes, floor tiles etc…) shall be performed inside the DIIDC unless special arrangements are made.
- Employees shall only access racks that contain equipment for which they are personally responsible.
- All persons must stay in their designated area.
- No person is to interfere with any equipment not managed by them.
- No person is to interfere with data center operations.
- Only DIIDC staff shall access the sub-floor or remove floor tile.
- All persons must wear their ID and it must be visible at all times.
- All problems and/or concerns will be communicated to the DIIDC staff.
- In the event of an emergency, notify DIIDC staff immediately.
- All areas, including workstation, will be kept clean and organized.

12.1.8 Equipment

DII

In order to enhance security and reduce the chance of disruptions, the following policies apply to all equipment housed in the DIIDC.

- An equipment form must be completed for all equipment installations and removals.
- Equipment forms can be obtained online or by contacting the DIIDC Manager.
- DIIDC employees will deny access to anyone who intends to install or remove equipment without an installation form on file.

The DIIDC is intended to be a limited physical access location for servers. Systems administrators of machines, which are housed in the DIIDC, must plan their servers as if they

will only get physical access to them when it is necessary to perform hardware modifications or replacements.
Servers will be configured with secure access administrative tools to allow for remote maintenance. All machines in the DIIDC must be rack mountable.
All new systems to the data center must undergo a security scan or audit prior to install. While the DIIDC provides increased network security, it is still necessary to take care of host-based security policies. Hosts in the DIIDC will be scanned regularly for vulnerabilities and those reports provided to the appropriate personnel. A security plan must be submitted to the DIIDC manager.

All new systems and hardware to the DIIDC will need to be coordinated and scheduled with the DIIDC staff.

NO equipment may be placed outside of the designated rack.
NO objects may be placed on top of or next to a rack on the floor.

Portable Equipment

Portable equipment such as notebook computers should be fitted with locks designed for notebooks, and secured to a desk whenever possible.

- Unattended notebooks and portable equipment will be stored in a locked cabinet or room.
- Notebook computers will not be left in vehicles unless locked in the trunk out of view.
- Notebook computers will be protected from excessive heat and cold.
- Notebooks will be returned to the home clinic after use at remote clinics.
- Notebooks or portable devices will not be serviced or sent to surplus unless authorized by AHS IT.
- Only State of Vermont authorized notebook computers with ability to encrypt data will be used for remote WIC Clinics.

12.1.9 National Life Additional Data Center Rules (DII NLDC)

Access

- National Life issued photo access card is required for access.

Equipment

- Do not carry any equipment larger than a laptop.
- For larger equipment, please contact National Life Security for separate entrance access. Please allow 24 hours advanced notice.

12.1.10 Hardware/Software Maintenance & Upgrades of Production Equipment

- Authorized personnel may perform maintenance and/or repairs on equipment on an as-needed basis as approved by the DIIDC Manager.

12.1.11 Network

The DII Network Engineering (NE) has the primary responsibility for the design, service and management of the State of Vermont’s Wide Area Network (WAN), Metropolitan Area Network (MAN) and Data Center network infrastructure. The group interacts with all State entities providing connectivity solutions for all site locations with an expected standard of 99.99% availability.

Network Engineering works in conjunction with State agencies and departments to design connectivity solutions to ensure business and system performance requirements are met. NE functions in a unique position as the mid-point to all State of Vermont network communication.

This central vantage point allows NE to provision end-to-end service needs for large projects as well as be a valuable resource to departments needing network assistance or diagnosing LAN events. One such service is a “virtual” firewall service that is a unique offering for departments without the need to purchase additional hardware.

Network Engineering monitors and manages the daily operations and network health from a centralized operations center in Montpelier and works at levels II and III of the triage process within DII. Service and project requests are processed through a centralized work order system to efficiently route work requests to the appropriate team. The NE group also provides network/system monitoring and alerting services for departments and provides a custom department monitoring web portal.

DII Network Engineering

- Maintains DNS services for a majority of the State of Vermont’s domains
- Maintains several layers of network firewall systems
- Maintains monitoring services that continually watch the stability of the State’s Network Infrastructure.

These systems are capable of monitoring not only network equipment but also systems like HVAC, UPS, power distribution units, Servers, phone systems, etc. With these systems, Network Engineering creates monitoring portals and alerting services for agencies and departments to present a single status tool for their network health.

Network Engineering also employs Intrusion Detection Systems (IDS) and other systems that monitor potential hostile traffic on the network. These systems can be leveraged for compliancy and security enforcement.

Purposes for monitoring systems:

- Stability of systems and services running on the network both Local Area Networks (LAN) and Wide Area Networks (WAN).
- 24 / 7 / 365 alerting of events to create efficiencies of not staffing around the clock.
- Mean Time to Recovery (MTTR) is significantly reduced when devices are monitored to show timing, and relationships of alerts.
- Compliancy to regulatory guidelines often requires monitoring at several layers to be in compliance.
- Automated response to monitored events is critical in maintaining stability through malicious attacks. Without monitoring and evasive action taken promptly, a domino affect can cripple network environments.

12.1.12 State Continuity of Operations Plan (COOP)

State of Vermont COOP plans are available at www.VermontCOOP.com via secure access.

13 Application Level

13.1 Environment Security

All WIC Local Agency physical locations are within one of the 12 State of Vermont District offices and governed by the State of Vermont Agency of Human Services Policies and Procedures as well at State of Vermont Policies and Procedures.

- Locations are climate controlled
- Locations have lockable closets and cabinets for EBT Card stock and equipment security
- Equipment located in areas accessible to clients and/or the public will be properly secured to prevent tampering or accidental interruption of service.

- AHS network automatically logs off a user after a specified period of inactivity
- Vermont Department of Buildings and Grounds (BGS) maintain Security for the District Office Buildings, which have electronic key lock entry
- Users logoff or turn off their computers/workstations when they will be away for any period of time
- Computers/workstations, servers and telecomm closets are kept clean and free of dirt, dust, and food
- Components are protected by surge protectors or line conditioners

Disaster Emergency Action Policy
Disaster Emergency Action Policy is governed by BGS and located here - http://bgs.vermont.gov/sites/bgs/files/pdfs/security/BGS-SEC-Vermont-ASAP-Manual.pdf

District Office Disaster Recovery
Disaster Recovery is captured in the State of Vermont COOP plan and certain specifics are particular to each location, however the following apply to all locations:

- Key Access Card Reader System – The ProWatch Database handles the card reader key system in multiple buildings throughout the State. Card readers store information (can be disconnected from the network) and the card readers will still work. The File Server is in a DMZ -- behind a firewall. The system is backed up nightly and tapes stored off site.
- Exchange Email System -- DII Exchange email system for multiple departments and agencies This email system is backed up and maintained by the Department of Information & Innovation.
- Telecommunications – The Centrex phone system for State Government & all district offices This system is maintained by the Department of Information & Innovation.
- Wide Area Network (WAN) - The data circuits that connect Vermont's Wide Area Network provides network connectivity and Internet access for all district offices. The Department of Information & Innovation is responsible for maintaining and backing up this network.
- IT databases - All IT databases are on secure servers at DII or VDH.

Each location's COOP maintains the following:
Annex A - Teams and Responsibilities
Annex B - Alternate Facilities
Annex C - Mission Essential Functions
Annex D - Orders of Succession
Annex E - Delegations of Authority
Annex F - Alert Notification Procedures
Annex G - Vital Records / Resources
Annex H - Drive-Away Kits
Annex I - Communications
Annex J - Security Access Control
Annex K - Family Disaster Plan
Annex L - Devolution
Annex M - Test, Training, and Exercise
Annex N - Facility Evacuation
Annex O - Contacts Roster
Annex P - Pandemic Planning
Annex Q - Risk Assessment
Annex R - Risk Specific Action List

13.2 Internet/AHS Network Security

All District Office Clinics have web access via the AHS network. The network has a robust set of monitoring tools including On-access McAfee Scanning using the Enterprise Edition. Laptops used for remote locations will have state virus control installed. The antivirus software is configured so that virus definition automatically update without user interaction. AHS IT has the responsibility to assure firewall protection.

13.3 AHS/DII Helpdesk Operations

Both AHS and DII have Helpdesks available by e-mail or phone, with ticket functionality for IT problems. The response time to tickets is tracked for constant improvement. Specific ticket problems are routed to the subject matter expert (SME).

13.4 Separation of Duties

Role based

- All users will log into the Vermont State Network with State supplied credentials.
- The system must employ a role-based security that allows user access to application functional areas based on user security level. Roles will include but not be limited to public (For applications, etc), Clinician, DO admin. State Admin.
- The system will allow users to have more than one role.
- The system administrator will be able to add and edit permissions for system access.
- The system will have the ability to support file, record and field level security.
- Security will be available to all modules and integrate with network operating security

13.4.1 Create Role Profiles

- The system must employ a role-based security that allows user access to functional areas based on user security level. Roles will include but not be limited to public (For applications, etc), Clinician, DO admin. State Admin.
- The system will allow users to have more than one role.
- The system administrator will be able to add and edit roles for system access.

13.4.2 Create User Profiles

- The system will have the ability to support various levels of access by authorized users.
- The system will allow users to have more than one role.
- The system administrator will be able to add and edit permissions for system access.

13.4.3 Passwords

Password standards are set at the State level by DII.

Password Development

- Service account passwords will be changed a minimum of every sixty (60) days.
- Service account passwords shall be a minimum length of eight (8) characters in a combination of upper and lower case alpha, numeric, and special characters.
- Default vendor passwords shall be changed during or immediately after installation of the information system product.
- Password changes shall be systematically enforced where possible.
- Accounts shall be systematically disabled after ninety (90) days of inactivity to reduce the risk of compromise.

System Password Protection

- Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at a system password to any unauthorized person(s). Since systems are managed by more than one person, passwords shall be administered on a need-to-know basis only. If system passwords are "predetermined or sequential" they are to be kept locked in a secure area at all times.
- Passwords shall not be transmitted electronically over the unprotected Internet, such as via e-mail.
- No employee is to keep an unsecured written record of passwords, either on paper or in an electronic file unless kept in a controlled access safe or an encrypted file.
- If an employee either knows or suspects that a system password has been compromised, it must be changed immediately and reported to the IT department manager.
- If an employee terminates employment, it is necessary to change system passwords that the employee has knowledge of. Each agency/department is responsible for documenting these requirements within their written procedure.

All users of the MIS system are state employees and currently trained in the above procedures and rules.

13.5 Data Integrity

13.5.1 Data Conversion

Data conversion is the responsibility of DII who hosts and maintains the current WIC application. All conversion activities will occur within DII physical security and under DII security Policy and Procedures.

13.5.2 Data Entry

Data integrity at the WIC clinics will be maintained at both the record and field levels within the centralized database. Data input will occur mainly at the Clinic level and proper training is imperative to maximize data integrity.
All staff scheduled to use the system will receive intensive training. Training will lessen the risk for erroneous data entry or accidental misuse that might compromise data integrity. For more information, refer to the Training Plan.

13.6 Patient Privacy

Computer monitors will be located to allow viewing by authorized personnel and participants but positioned to eliminate viewing by unauthorized persons.

13.7 Performing Backups

The system will save a backup of production data hourly and make the data available for immediate restoration for 30 days after the date/time of each back-up. The backups will be stored on media for off site storage after 30 days.

Backup and recovery services are provided by NetBackup, which can be managed by designated NetBackup System Administrators. The NetBackup application and database components are installed on separate servers (Master & Multiple Media Servers), plus a HP MSL4048 2 Ultrium960 Tape Drive, in the SOV Enterprise NetBackup Environment, as part of an HP EVA 8000.
SOV Enterprise Backup/Recovery Services provides a complete and flexible data protection solution for a variety of platforms, including Microsoft Windows, UNIX, Linux, and NetWare systems. Also included is the support for leading database engines like Microsoft SQL Server, Sybase and Oracle; providing near real time database protection.

14 EBT Retail Level Security

Point of Sale (POS) Terminal security

Participants access to their benefits through POS terminals located at WIC authorized retailers. Benefit transactions performed through online processing will use a central processor to verify PINs and authorize transactions. Retailer requirements include cashier ID and password verification, settlement controls and integrity of transmitted data.

15 Information System Security Plan Completion Date

12/15/2011

16 Appendix A: Glossary

133DC	133 State Street Data Center
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency - AHS	Agency of Human Services
AOT	Agency of Transportations
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The quality or condition of being authentic, trustworthy, or genuine.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Availability	Ensuring timely and reliable access to and use of information.
BDC	Barre Data Center
BGS	Building & General Services, Department of
Chief Information Officer	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Common Security Control	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information

	system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications before, during, and after system implementation.
COOP	Continuity of Operations Plan
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
DII	Department of Information & Innovation, State of Vermont
DIIDC	DII Data Centers
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner(or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

L3DC	Level 3 Data Center
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
National Security System	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
NLDC	National Life Data Center
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Privacy Impact Assessment	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
Record	Any written or recorded information, regardless of physical form or characteristics, which is produced or acquired in the course of agency business
Remote Access	Access by users (or information systems) communicating external to an information system security perimeter.
Remote Maintenance	Maintenance activities conducted by individuals communicating external to an information system security perimeter.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from

	the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Control Baseline	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Impact Analysis	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.
Security Label	Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.
Security Objective	Confidentiality, integrity, or availability
Security Requirements	Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer	DII Official responsible for carrying out Statewide Information Security
SOV	State of Vermont
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
System-specific Security Control	A security control for an information system that has not been designated as a common security control.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Agent/Source	Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability.
Threat Assessment	Formal description and evaluation of threat to an information system.
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.
User	Individual or (system) process authorized to access an information system.
VDH	Vermont Department of Health
Visitor	An employee who does not work in the DIIDC; An employee who does not possess authorization to the DIIDC; A person who is not an employee of the State of Vermont.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.

17 Appendix B: References

Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

“NIST Guide to Information Technology Security Services”, *National Institute of Standards and Technology* Special Publication 800-35, Oct. 2003. Web. 10 Oct 2011 <http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf >

"SPIRIT Systems Documentation." *USDA FNS*. USDA, 06/09/2010. Web. 9 Aug 2010. <http://www.fns.usda.gov/apd/library/spirit_docs.htm >.

State of Vermont. Department of Information and Innovation. Policy Central. Montpelier:, 2011. Web. < http://dii.vermont.gov/Policy_Central>.

"WIC EBT Document Library" *USDA FNS*. USDA, 04/06/2010. Web. 9 Aug 2010. <http://www.fns.usda.gov/apd/library/wic_ebt_docs.htm >.

18 Appendix C: DII SOV Policy

- Backup Policy
- Change Control Policy
- Electronic Messages Best Practice for All Public Agencies (2009)
- Electronic Signature Guidelines
- Electronic Signatures -- Best Practices

- Electronic Signatures Best Practice for All Public Agencies (2010)
- Incident Response Policy
- Information Security Best Practice for All Public Agencies (2009)
- Information Security Policy
- Intrusion Detection and Prevention Policy
- Malicious Software Protection
- Minimum Security Standards for Application Development Policy
- Physical Security for Computer Protection - Policy
- Source Code Requirements for Business Applications
- System/Service Password Policy
- Third Party Network Connectivity
- User Password Policy and Guidelines
- Wireless Communications

19 Appendix E: EBT Host Disaster Recovery Plan

*To be included when contracted with EBT Services Provider

20 Appendix F: WIC System Disaster Recovery Plan

*To be included when contracted with T&I MIS Contractor

21 Appendix G: Site Plan

*To be included when contracted with T&I MIS Contractor